SIEMENS

Siemens Corporation
Corporate Technology

Secure & Resilient Functional Modeling for Navy Cyber-Physical Systems

FY17 Quarter 1 Technical Progress Report

DoD sponsoring/monitoring agency: Office of Naval Research
875 North Randolph Street
Arlington, VA 22203-1995
Contract number: N00014-16-C-2005
Period: October 1, 2016 – December 31, 2016
Total contract amount: $932,742
Costs during period: $41,566
Costs to date: $41,566
Estimate to complete: $932,742

Summary

The project was started in this quarter. A kickoff meeting was held on September 26-27 in UCI, where the participants revised the proposal text together in order to ensure a common understanding of the project content and goals. The document "2016-09-26_ONR_Kickoff_Meeting_UCI.pdf" contains the minutes of this meeting.

Work has begun on the work packages Functional Editor and Attack Generator, with preliminary work on the Functional Modeling Compiler work package.

On November 9, Siemens requested that ONR make a determination that all tasks and work to be performed by Siemens and by UCI under this contract is fundamental research, because a determination of fundamental research by the Contracting Officer is necessary prior to execution by UCI of any resulting award containing any agency clause restricting the disclosure of information or freedom to publish. ONR issued the requested determination on December 19. As a result, UCI was formally unable to execute the work as planned for this quarter. These delays will be accounted for in the project plan.

Project Goals for this Quarter

- Define and propose a concrete use case for the project. (Siemens)
- Define the attack models that will be used throughout the project. (UCI)

Progress and Achievements

Work Package	Status	Technical Achievement	Milestones and Deliverables
Attack Generator (UCI)	Late start due to subcontract negotiation.	Started initial study of cyberattacks and attack models. Started definition of attacks.	Pending.
Functional Editor (SCCT)	Started, on track.	Started development of web-based editor for functional models. Designed database to store functional models.	Pending.
Functional Modeling Compiler (SCCT)	Started, on track.	Defined the tool's scope and functionality. Identified implementation techniques.	Pending.

Work Package	Status	Technical Achievement	Milestones and Deliverables
Simulation Engine (SCCT)	Not started.		
Agent-based Distributed Runtime (UCI)	Not started.		
Model Management Backbone (SCCT)	Not started.		

Technical Details

Navy Use Case

In order to evaluate the effectiveness of the functional modelling approach for integrating cybersecurity into the development of Navy ship control systems, it was determined that this project will employ the model of a Ship Chilled Water Distribution System as a central use case. This model represents a part of the fluid and electrical system of a Navy ship, and the schematic of its fluid subsystem is shown in Figure 1. The main purpose of the system is to provide cold water from coolers (chillers) to heat loads, in order to regulate their temperature and maintain it within suitable operation conditions. The fluid subsystem model includes 4 main component types: loads, chiller plants, valves, and pipes. The plant has a total of 4 zones, and there is one chiller plant per zone. The electrical subsystem features 8 redundant power panels to supply power to the 4 zones. The control logic for the model system shall maximize the operability and the survivability of the system. As a second goal, the control logic shall maximize the efficiency of the system's operation.

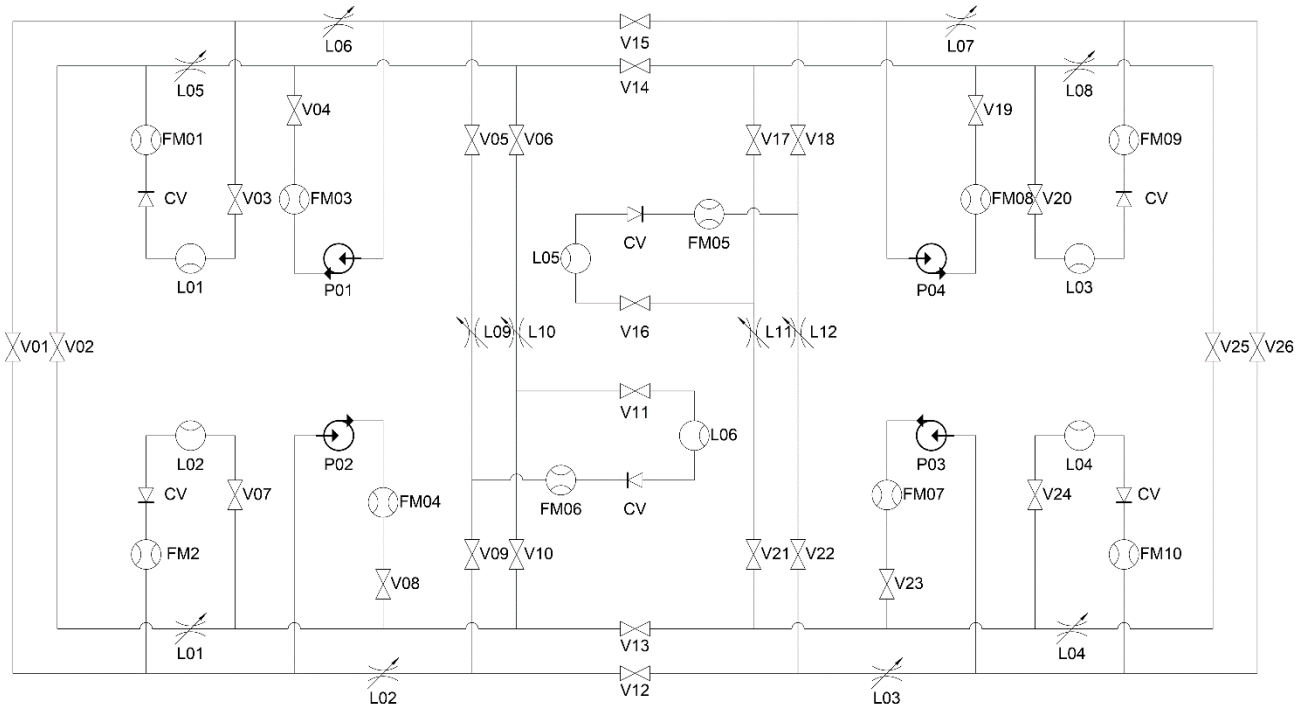

Figure 1: Fluid subsystem

In the envisioned scenario, the Ship Chilled Water Distribution System Model will be subject to cyberattacks in a modeling and simulation environment. The goal of this evaluation is to show the effectiveness of including cybersecurity aspects in the early design phase of the system. Cyberattacks may be carried out by an attacker by disrupting or disabling the operation of sensors or actuators, or by gaining access to the control system remotely and modifying control parameters in order to disrupt the operation of the controlled system.

Attack Generator

The attack classes that will be studied in the project are those targeting the integrity and the availability of the system. Attacks targeting data confidentiality are out of the scope of the project. The vectors for cyberattacks that will be considered in this project were delimited to sensor tampering, actuator tampering, and parameter tampering. Attacks involving high-level digital communication between the ship and external systems will be considered out of scope for the project, as well as the high-level interference with the digital communication inside the ship.

UCI started a technical study by exploring existing articles related to cyberattacks affecting the Navy and military targets in general, as well as current research aiming at resilience against these kinds of cyberattacks (e.g. software and system diversification techniques, isolation and restoration techniques, separation of information for protection against side channel attacks).

For the design of the attack models, UCI has taken previous work as a starting point and is considering the defined use case for developing the detailed model.[1] The attack objectives are being selected and defined based on the plant model from the use case, e.g. safe use of pumps and valves (overflow, defeating interlocks) or overheating of the loads (defeating the control strategy). The attack models that are currently being developed are:

1. Basic attack models
    a. Fuzzy attack
    b. Interruption attack
    c. Man-in-the middle attack
    d. Replay attack
    e. Overflow attack
    f. Down-sampling attack
    g. Control parameter attack
2. Complex attack models
    a. Attacks on temporal domain survivability
    b. Attacks on spatial domain survivability
    c. Attacks on adjacency matrix

Functional Editor

The development of the Functional Modeling Editor (FME) was started in this quarter by SCCT. The tool consists of a web-based editor for functional models, which is paired with a database that is used to store these functional models. The web application is being developed in HTML5 and JavaScript, and uses Node.js as the server-side runtime system. The database for the functional models is based on MongoDB and was designed using an object-oriented data model. The use of these platforms allows the system to be portable across different operating systems, and adds the possibility of a future deployment to a cloud-based architecture.

Some of the features offered by the FME are:

- Hierarchical block system for structured and scalable modeling of large systems.
- Support for different kinds of graphically-distinguishable blocks (functional, system context, cyberattack, cybersecurity function) and connection ports.
- Model editing with flexible selection and modification of block and port types.
- Automatic drawing of block connections.
- Graphical highlighting of invalid connections.
- Generic block attributes for effective modeling specific components and systems.

The FME is currently in development. A first version is expected for the next quarter.

Functional Modeling Compiler

SCCT has also taken the first steps towards the development of the Functional Modeling Compiler (FMC), by defining the tool's scope and functionality. The FMC will translate the system model, the cybersecurity model

[1] The design of the attack models was postponed during this quarter in order to wait for the pending determination about fundamental research from ONR. This task was resumed as soon as this issue was resolved.

and the attack model to simulation models for their evaluation in the simulation environment. The procedure for mapping functional models to simulation models will include the partitioning of the functional model, the generation of interfaces between the simulation components and the selection of the components for their instantiation in Amesim and Simulink.

Presently the envisioned FMC will use the following techniques in order to fulfill its tasks:

- Employ a model transformation engine in order to implement the functional mappings.
- Perform structural modifications to the generated models and control programs in order to implement added cybersecurity functions, e.g.:
    - Add redundant structures.
    - Add alternative signal sources and signal selectors.
    - Add plausibility checkers.
    - Introduce system partitioning and isolation.

The development of the FMC will continue during the next quarters of the present fiscal year.

Future Work

The project work intended for the next quarter consists of the following tasks:

- Definition and design of the attack models. (UCI)
- Preparation of the first version of the FME with basic functionality. (SCCT)
- Development of the FMC. (SCCT)
- Initial definition of KPIs for assessment of the effectiveness of the technical approach. (SCCT)

Points of Contact

Technical	*Administrative*
Dr. Gustavo Quirós Siemens Corporation, Corporate Technology 755 College Road East, Princeton, NJ 08540 Phone: (609) 216-5497 gustavo.quiros@siemens.com	Mr. Samuel Roods Siemens Corporation, Corporate Technology 755 College Road East, Princeton, NJ 08540 Phone: (609) 734-3575 samuel.roods@siemens.com